Taylor & Francis
Taylor & Francis Group

Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: http://www.tandfonline.com/loi/tbit20

Self-reflection on privacy research in social networking sites

Ralf De Wolf, Ellen Vanderhoven, Bettina Berendt, Jo Pierson & Tammy Schellens

To cite this article: Ralf De Wolf, Ellen Vanderhoven, Bettina Berendt, Jo Pierson & Tammy Schellens (2016): Self-reflection on privacy research in social networking sites, Behaviour & Information Technology, DOI: 10.1080/0144929X.2016.1242653

To link to this article: http://dx.doi.org/10.1080/0144929X.2016.1242653

BEHAVIOUR & INFORMATION TECHNOLOGY, 2016
http://dx.doi.org/10.1080/0144929X.2016.1242653

Taylor & Francis
Taylor & Francis Group

Self-reflection on privacy research in social networking sites

Ralf De Wolf[a,b], Ellen Vanderhoven[c], Bettina Berendt[d], Jo Pierson[a] and Tammy Schellens[c]

[a]Department of Media and Communication Studies (Iminds-SMIT-VUB), Vrije Universiteit Brussel, Brussel, Belgium; [b]Department of Communication Sciences (Cepec, Iminds-MICT-Ugent), Ghent University, Ghent, Belgium; [c]Department of Educational Studies, Ghent University, Gent, Belgium; [d]Department of Computer Science, KU Leuven, Heverlee, Belgium

ABSTRACT

The increasing popularity of social networking sites has been a source of many privacy concerns. To mitigate these concerns and empower users, different forms of educational and technological solutions have been developed. Developing and evaluating such solutions, however, cannot be considered a neutral process. Instead, it is socially bound and interwoven with norms and values of the researchers. In this contribution, we aim to make the research process and development of privacy solutions more transparent by highlighting questions that should be considered. (1) Which actors are involved in formulating the privacy problem? (2) Is privacy perceived as a human right or as a property right on one's data? (3) Is informing users of privacy dangers always a good thing? (4) Do we want to influence users' attitudes and behaviours? (5) Who is the target audience? We argue that these questions can help researchers to better comprehend their own perspective on privacy, that of others, and the influence of the solutions they are developing. In the discussion, we propose a procedure called 'tool clinics' for further practical implementations.

ARTICLE HISTORY
Received 18 May 2016
Accepted 20 September 2016

KEYWORDS
Social networking sites; privacy; self-reflection; human rights; science and technology studies; tool clinics

1. Introduction

Social networking sites (SNSs) have not only become a part of the everyday acting repertoire for many, but they also challenge the management of personal information flows and the notion of privacy (Xu 2012). The difficulties of these processes have spurred a large body of research on the many faces of privacy, coming from a wide range of scientific, political, economic, and other perspectives. Such work, however, cannot tread a linear way to the one truth and the one solution to all problems. On the contrary, the more these perspectives meet and interact with one another, the clearer one all-too-often-forgotten truth about research shows itself: no researcher is just a neutral collector of facts; the critical questioning of one's own approach is often crucial for progress. With this approach, we aim to contribute to making privacy research more effective – because only through being transparent and self-reflective about our own practices can we help bring privacy into being.

In the course of working together in a large interdisciplinary project,[1] we repeatedly observed misunderstandings and confusions both in our own collaboration and in the literature. We compiled the most frequent sources of these misunderstandings and confusions and distilled them into the five self-reflective questions. These questions are used to structure, describe, and discuss the assumptions and implications behind the decisions made in the research process. This approach is not the only way in which this could be done, and we neither can nor intend to tackle all issues. To be precise, much research has been devoted to developing privacy solutions and/or designing technologies while taking into account users' privacy (i.e. privacy by design). In this paper, our goal is to zoom out and make the relation between the researcher and the technology under development (privacy solutions) more transparent.

The paper is organised as follows. First, we frame our approach and provide an overview of the self-reflective questions. Second, we discuss how privacy problems are defined, investigate which actors are involved in this phase of definition, and ask whether privacy is perceived as a human right or as a property right on one's data. Third, we focus on the solution for a problem defined earlier and discuss the issues related to increasing awareness and changing attitudes and behaviours. Finally, in the discussion, we propose a procedure called *tool clinics* for further practical implementations of the proposed approach.

2. Five self-reflective questions

When developing technologies, researchers always have a certain set of ideas, norms, and values that they put into their technologies (Williams and Edge 1996;

CONTACT Ralf De Wolf ralf.dewolf@ugent.be

Hackett et al. 2008; Gillespie, Boczkowski, and Foot 2014). Moreover, the role of a researcher has extended from a 'neutral' collector of facts with a focus on scientific progress to a socialisation agent with a society-oriented goal. Increasing digital skills, facilitating control over personal information, and raising awareness about privacy threats are but some of the goals privacy researchers could hope to attain in addition to gathering and analysing data. Because of the non-neutral role of researchers and their non-neutral solutions, we consider it important to make the decisions made in the research process transparent. Five questions will be discussed in the following sections to help reach that goal.

We structured the paper in a way similar to the stages in which a solution for a privacy problem typically proceeds: defining the problem and developing a solution. It appears self-evident to first define a problem and then solve it. But in the definition of a research problem, researchers are strongly influenced by their own goals, values, and pre-conceptions, and any solution they choose will also be influenced by the properties of the 'solution technology', be that a certain type of discourse, a software tool, or the context defined by the institutional setting and the people in it. So in the Latourian sense, the first phase (problem definition) will be strongly influenced by the 'human' in the 'human-apparatus' system, and the second phase (problem solution), by the 'apparatus'.[2] We argue that it is necessary to make these design choices more transparent, and we will provide five self-reflective questions as leads into making the problem definition phase (Qs 1 and 2) and, respectively, the problem solution phase (Qs 3–5) more transparent.

2.1. Q1. Which actors are involved in formulating the privacy problem?

The way the privacy problem is defined depends on the actors and stakeholders that are involved. The first self-reflective question has two aspects: (a) 'what relationships does it concern?' (i.e. relationships towards other people or towards institutions) and (b) 'which actors define the privacy problem?' (i.e. security experts or users).

SNS users disclose information to multiple actors. This has implications for the definition of the privacy problem. Raynes-Goldie (2010) differentiates between institutional privacy, that is, privacy vis-à-vis third parties like commercial institutions, governments, and the like, and social privacy, that is, privacy vis-à-vis other people like family, friends, and acquaintances. Social privacy problems tend to be more visible than institutional privacy problems and originate from everyday social interaction between SNS users, such as embarrassing footage being (re-)shared by Facebook friends. Here, privacy is a means for achieving something else, like self-realisation, intimacy, or solitude (Westin 1967). The problems here are mostly contextual by nature. In the current digital and networked society, temporal, spatial, and social boundaries are becoming more fluid (Bauman and Lyon 2013), which creates dynamics such as a merging between the public and private sphere, context collapse, and invisible audiences (boyd 2008a). Institutional privacy problems concern the watching, gathering, processing, and using of personal information by third parties. Users are often not aware of these background processes related to their personal data (Acquisti and Gross 2006), which can explain why they often do not express any concerns with regard to this matter.

The definition process also depends on who defines the privacy problem. Gürses and Diaz (2013) identified two large groups of viewpoints in the privacy literature. They characterise one of them as expressing a notion of privacy largely defined by 'security experts': scientists or developers of privacy-enhancing technologies (PETs), mostly from a security-and-privacy background. PET developers tend to focus on the data processing and use. Martin, Rise and Martin (2015) showed how IT professionals are particularly sensitive to securing data from unknown third parties. Some of them extend this by questioning the ongoing commodification of personal information and surveillance (e.g. Gandy 2003; Coté and Pybus 2007; Fuchs 2012). The other group is characterised as expressing a notion of privacy based on user perceptions. This relates to the concerns that user's express and to the harms that they experience when technologically mediated communications disrupt social boundaries. In terms of the distinction made by Gürses and Diaz (2013), the 'security experts' focus mostly on institutional privacy, while the 'users' tend to focus on social privacy.[3]

We argue that a researcher should question which actors are involved when defining the privacy problem. Both social and institutional privacy problems concern the disclosed information in SNSs, but they typically involve different actors and require different solutions. Moreover, they face different challenges, as indicated below.

Social privacy problems are strongly connected to the everyday practices of users. Practices that were once thought to be privacy violations can become normal and thus taken for granted. The emergence and acceptance of the Newsfeed can serve as an example. In September 2006, Facebook introduced the Newsfeed, a constantly updating start page that displays the actions of users performed on Facebook for a wider audience,

that is, pages they like, conversations they have with others, comments, or music preferences. Although CEO Mark Zuckerberg stated that no privacy was violated, boyd (2008b, 18) argued that the sense of control over information was harmed because information was reused in a way that users had not foreseen. Initially, many users protested against this feature (boyd 2008b). Nowadays, for most the Newsfeed does not appear to be a privacy violation, but a central part of the SNS experience. Since social privacy problems are closely connected to everyday practices, these practices can limit our view on privacy and its (changing) meaning. This could even lead to an unquestioning acceptance of the privacy policy of service providers.

Institutional privacy problems focus on the gathering and collecting of the digital footprints that users leave behind. When a solution is proposed – for example, to encrypt the traffic between users and service providers – it might well be that the postulated 'problem' is not perceived as such by users. However, that something is perceived as a problem by users is a pivotal factor for a subsequent solution to be adopted and appropriated.

2.2. Q2. Is privacy perceived as a human right or as a property right on one's data?

The discussion in the previous section has already given a glimpse on the fact that even among experts privacy remains a contested term. There is a general agreement that privacy is inherently relational, where the type of 'other' in the relationship can be one basis for classifications (e.g. into social and institutional privacy, as explained above). But beyond that, the term has very different interpretations, which may or may not be mutually exclusive. We will highlight important interpretations by structuring key notions of privacy along three dimensions, and then argue why we believe the researcher's stance on *what the right to privacy is* to be a better candidate for a self-reflective question than his or her position in this multidimensional landscape of *what privacy is*.

One important distinction is that between privacy as intimacy and 'the right to be let alone' (e.g. Warren, Samuel and Brandeis 1890) and privacy as autonomy, including informational self-determination and its control of data about the self (e.g. Westin 1967). Another popular definition underlines the important role of a protected sphere as a space for autonomy, and it shifts the focus from control to self-realisation: 'the absence of unreasonable constraints on the construction on one's identity' (Agre & Rothenberg 2001). In emphasising the role of privacy for other goals rather than for its own sake, this definition is also related to the notion of the 'instrumental' role of privacy for other goals such as freedom of speech and democracy (e.g. Rouvroy and Poullet 2009). These two notions of instrumentality differ along another dimension, that of individual vs. collective. For example, social psychologists Altman (1976) and Petronio (2002) have focused more strongly on the individual level, when compared with scholars such as Nissenbaum (2004), who in her proposal of 'contextual integrity' has focused on the social norms governing what actors and what (re-)contextualisations are deemed appropriate.

Opinions also differ along a third dimension: whether privacy can be regarded as an invariant human need and behaviour that can be observed across times and cultures (e.g. Altman 1976), or a relatively recent concern brought about by the emergence of modern media. The latter is sometimes suggested with reference to Warren and Brandeis' (1890) seminal discussion of the modern legal notion of the right to privacy, which derived from a court case involving the then new medium of photography – see however Greenwald (2014) who identifies privacy legislation ideas in the Code of Hammurabi, which can be argued to support the 'invariant' view.

In the current paper, we are not trying to contribute to this discussion, and we believe it is a matter of standard scientific practice for researchers to know and state their definition(s) of what privacy *is*. We believe, however, that – based on their descriptive definition(s), but in no way following from them in a straightforward way – researchers also bring normative notions to bear: what privacy *should* be. Obviously, this stance has a large impact on the solutions researchers will propose (Qs 3–5). However, we observe that researchers are often much more implicit regarding this normative choice than regarding the descriptive one. And because this aspect is important but often remains in the background, we consider the question to be an important recommendation for our list of self-reflective questions.

So what exactly does it mean to have privacy rights? We want to summarise – in a necessarily simplified way – the current discussion in terms of a spectrum between two perspectives. These can best be described by the rallying cries 'my data belong to me, and I can use it for whatever purpose' vs. 'privacy is a human right, and its protection is in the public interest'.

Both perspectives talk about (among other things) a subjective right: an entitlement that a person has, and neither presupposes any obligation (so neither says that people are forced to opt for privacy). However, they differ in many aspects. The perspectives are loosely aligned with different legal regimes: property rights on personal data vs. privacy (and data protection) as a fundamental right, that is, as a human right guaranteed by a

constitution (similar to, e.g., the freedom of speech). The perspectives are also aligned with different economic/political regimes: economic liberalism with its focus on individual freedoms and markets vs. social liberalism with its (added) focus on differences between people regarding power, wealth, education, and other factors (and the need to address these in the interest of social justice); interdependencies between individual decisions; and the resulting market failures and needs for regulations. Due to the proliferation of legal and economic variants that are being proposed, we will refrain from an in-depth legal or economic analysis and instead group them into two (necessarily idealised) perspectives, call these the *data as individual property (DIP)* perspective and *privacy as a human right (PHR)* perspective, and explain the perspectives by the positions they take on a number of key issues.

We argue that an answer for each of these issues or sub-questions can help in making one's perspective on privacy transparent.

1. Who gets to *decide* what happens with personal data? This question is often framed as one of 'individual choice vs. collective regulation'. DIP proponents argue that individuals know best what is good for them, differ in their preferences (including their desired level of privacy), and should therefore decide. They observe that 'in existing system architectures, users have little control over what information is being shared [,] and [they] must trust the service providers to protect their highly individualised and sensitive data' (Mun et al. 2010). In other words, DIP proponents perceive the current situation less as one governed by data-protection regulation, and more as essentially ungoverned. PHR proponents, on the other hand, emphasise that individuals may not always know what is in their best interest and that property-rights regimes too need regulation.[4] In addition, PHR proponents argue that social effects (see 6. below) should limit individual choice.
2. Can individuals profit (financially) from 'the data industry', for example by selling (access to or use of) their personal data? DIP proponents point to the huge gains made by data-processing companies; if people were enabled to 'own' their data, then they – the rightful owners – would be able to profit from this (Samuelson 2000). PHR proponents prefer to regard (personal and other) data as enablers of transactions that should be advantageous for people ('data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals', EU 95/94/EC, Recital (2)).[5]
3. May the right to privacy be *given away*? To a DIP proponent, this is a logical next step to best enable individuals to exercise control over their data and profit financially from tailor-made, individually negotiable deals: not only should individuals be able to 'sell their data', they should also be able to 'sell these data along with the rights on them'. Legally, this is the alienability of property rights. In contrast, human and fundamental rights are, by definition, inalienable: they 'belong' to a person anyway, they are constitutive of personhood, and they can thus not be given away or waived (Purtova 2010).
4. Can and should a (full-fledged) *market* in personal data exist? A DIP proponent would consider the steps of commodification (making data and the rights on them saleable and commensurable) as necessary on the route to efficient markets that make everyone better off. PHR proponents would argue that complete commodification is not possible anyway (see point 3.) and point to the many hidden (and, they argue, wrong) assumptions often made in arguments for commodification (e.g. Lohmann 2013).
5. Who is *responsible* for the protection of people's privacy interests? If privacy is a fundamental right (PHR), then the state is responsible for guaranteeing it – not only by not interfering with individual freedoms (negative right, 'freedom from'), but also by actively protecting them (positive right, 'freedom to', and the state's positive obligations). With DIP, on the other hand, people would be individually responsible for what they do with their data – thus, for example, if someone decided to sell all rights to his or her personal data, these rights would be gone as in the sale of a material possession or an intellectual product. The state would be responsible for protecting the property rights of the old as well as of the new owners.
6. What are the underlying assumptions about *individuals and collectives*? The DIP perspective focuses on individuals, in line with the general belief of economic liberalism that individual choice on markets will lead to the best global outcome. The PHR perspective more strongly perceives the challenges posed by economic and social inequalities and the questions of social solidarity as necessary starting points for political, economic, and legal designs. Related to this are beliefs about *interdependencies*. While DIP advocates tend to regard privacy as an individual question, PHR advocates emphasise the role of privacy for the public interest. In other words, one person's lack of privacy

may have unfavourable effects on everybody's fundamental rights and, therefore, on the very fabric of society.

Compromises between these two extremes are possible. As an example of a possible 'compromise' between the two idealised extremes of DIP and PHR, we briefly sketch some key elements of the European Union's legal treatment of privacy and data protection. On the one hand, the EU has made a firm commitment to privacy and data protection as fundamental human rights through the European Convention on Human Rights and the European Charter of Fundamental Rights (Articles 7 and 8) and a number of landmark judgements on these in courts (Purtova 2010; De Hert 2012). On the other hand, the basic template for data-protection law, the EU Privacy Directive EU 95/94/EC, explicitly set out to respect both (a) the interests and choices of citizens (see Recital (2) cited under point 2. above) and their fundamental rights and (b) the interests of commerce (for further details and arguments, see, for example, De Hert 2012 or Purtova 2010).

We believe that although some authors explicitly call for property rights on personal data (which, to the best of our knowledge, do not exist in any jurisdiction at the moment) and others explicitly investigate human rights issues, most researchers deal with different or more specific issues. Still, we argue that many specific issues would profit from a self-reflection on what assumptions lie behind them and what positions, economic interests, and political agendas may be furthered by them.

2.3. Q3. Is informing users of privacy dangers always a good thing?

Writing oneself into being online requires constant reflection (boyd 2008b; Markham 2013). The latter has been labelled with the term *ekstasis* (Waskul 2005). Markham (2013, 284) points out 'how everyday activities in digital media contexts require conscious deliberation, technical skills, and more reflexivity about activities or rules that are in constant play in the construction of self and society'. An essential part of such ekstasis is knowledge of the social situation. People, however, are often unaware of their online audience and/or its size (Bernstein et al. 2013; Litt 2013), or they do not differentiate between intended and unintended audiences among their online friends. Stutzman, Gross, and Acquisti (2013) point out that 'silent listeners', such as service providers and third-party applications, are often not even considered as an audience in the first place.

It would seem justifiable to make SNS users aware of their environment and outline both social and institutional privacy issues, so as to enable them to obtain a state of ekstasis. However, informing users or provoking awareness, we will argue, may also have negative consequences, is not always possible, and is biased by the view of the initiator.

1. Is awareness a value in itself? When growing up, we internalise the norms, values, and structure of the community and society we live in. They shape who we are and how we act in everyday life, a process that seems self-evident. New technologies and their related norms are also part of this environment and get domesticated and appropriated. When informing users of the dangers of SNSs and their consequences for the self, we also, to a certain extent, self-alienate them, that is, make them look at their own practices in relation to the environment. Internalising such an idea leads to a questioning of one's own behaviour and makes people think about their own actions, rather than act in the first place, which does not always contribute to a more enjoyable or easier life. Moreover, and in particular for SNSs, it may harm the positive reasons why users are on SNSs in the first place, such as developing identities, establishing bridging and social capital, and seeking information.

The assumption that having more knowledge is always better in all respects is thus not necessarily true. A researcher or designer who wants to inform users will have to trade off the risks of self-alienation or social displeasure against the risks that he or she wants to protect users from. In societies, we make these tradeoffs every day, assessing risks including 'that one wrong choice with irreversible consequences' differently, resulting in different urgencies with which we enforce self-alienation (or tolerate risk-taking), for example when it comes to alcohol, marijuana, heroin, drunk driving, or unprotected sexual intercourse. The assessment of these risks and the conclusions drawn for enforcement or tolerance are never just objective, statistical acts, but regularly involve a normative component.

Given the complexity of the architecture of SNSs and users' lack of knowledge about information processing by service providers, one could argue that it is necessary to make users aware of what is going on, so that they can make informed decisions. Users' capabilities, however, have been questioned from many angles. Acquisti and Gross (2006) indicate that bounded rationality affects the decisions users make, so that they do not always make decisions in their *best* interest, whatever that may be. Many experiments have demonstrated how users do not always act in line with their preferences and thus may make decisions that, even if they are informed decisions, do them more harm than good (Berendt, Günther, and Spiekermann 2005; Brandimarte, Acquisti, and Loewenstein 2012; Knijnenburg, Kobsa, and Jin

2013). If users still make the *wrong* choices when they are informed of potential privacy problems, when provided with the necessary tools to solve that specific problem, we should ask ourselves if awareness is always a value in itself.[6]

Making users aware of the dangers of SNSs presupposes that we *can* make users aware. In our second argument, we will illustrate how this is not always possible.

2. Is awareness possible? In premodern society, *when* was almost always inextricably connected with *where*. According to Giddens (1991), modern society is confronted with a 'time-space distanciation'. The latter, he argues, is a primary condition for the process of disembedding, which can be defined as dividing social relations from the local context in which they are embedded. As a result, we increasingly trust systems that we do not grasp completely. Following the conceptualisation of Giddens (1991), SNSs can be considered as such a system: it is complex to grasp the computational workings of SNSs and their effects on people's lives. Privacy is a multifaceted concept with many layers, consisting of intertwined notions that influence one another (Solove 2006). Privacy in a networked world is even more complex, as our discussion of the first lead question has shown. Giddens (1991) proposes to 'ride the juggernaut', that is, modernity, which is difficult because faceless commitment in abstract systems (e.g. trust in SNSs) is sustained by facework relations and re-embedded (e.g. friends explaining how to employ privacy settings), and internalising norms, values, and structures can make us unaware or, on the other side of the continuum, lead to self-alienation.

This brings us to our third argument: awareness does not automatically imply a questioning of communication technologies. We will illustrate how the views of users, non-users, and also researchers are naturally biased.

3. Is awareness neutral? Papacharissi (2012, 195) emphasises that 'historical context shapes how we interpret technologies. It informs uses, expectations, and rituals that are adjusted or re-invented'. It is unavoidable that SNSs are compared with previous communication technologies or previous experiences in general. Older generations or non-users will, therefore, not always understand why teenagers (or others) post information towards multiple audiences at once, while users who make use of SNSs on a daily basis will quickly appropriate its norms, values, and structures into their everyday practices. In other words, older generations or non-users limit their view by a nostalgic comparison with older technologies and experiences ('I didn't have a cellphone or Facebook to communicate with my friends, and I turned out fine'). Younger generations or older generations who make use of SNSs to extend their dramaturgical experience and keep in touch with their friends will be less critical of the technical properties of SNSs by means of appropriation. The differences between generations indicate how one's perspective is not neutral but situational. Similarly, raising awareness depends on the perspective of those who want to raise it, and who will justify their claims based on what they think are justifiable arguments.

Researchers could rely on how users make use of privacy settings provided by service providers to justify the need for raising awareness. However, in such an approach, the researcher does not question the privacy policy of service providers. Hence, via the authors' unstated assumptions, his or her views on privacy are largely similar to those of service providers. The ways we justify our goals can even be subtler. In a qualitative study, Wang et al. (2011) researched regrets in Facebook, with the aim of helping SNS users avoid such regrets. This can be valuable for users' reputation management or maintaining relationships with others. At first sight, it seems like a *neutral* and justifiable way of pushing users towards a course of action, presumed advantageous. After all, in this approach, the users themselves define what is appropriate and what is not, rather than the service providers. Nudging users based on what they would regret, however, is a very individualistic approach: are regrets and making mistakes not an essential part of human life?

As a consequence of these arguments about our third question, we ask researchers to be critical towards informing users. Rather than criticising transparency or awareness, we aim to criticise not being transparent about raising awareness. We argue that a researcher should justify why, how, and to what extent users should be made aware.

2.4. Q4. Do we want to influence users' attitudes and behaviours?

In addition to the question to what extent we want to inform the user and raise awareness about privacy risks in SNSs, the question should be asked whether the solution being developed aims at an attitudinal and/or behavioural change. When considering this question, one should keep in mind that developing solutions always includes a researcher's expectations of desirable attitudes and behaviour. This is not always in line with the goals and expectations of the user. It can be argued that every individual has the right to not care, and to choose to behave 'unsafely' if that is what he or she wants (e.g. given the benefits this entails).

It is understandable that privacy researchers believe they have the best interest of the user in mind when

they state that users should care about their privacy and behave as safely as possible. However, developing solutions in an attempt to influence users' attitudes and behaviour raises important ethical questions about the extent to which a researcher can impose his or her values (Kimmel 1988). Kelman (2001) suggested that statements such as 'it's for the users' own good' should be regarded as a violation of the principle of freedom. Indeed, forcing people to behave 'safely' in SNSs can be judged as paternalistic and even undemocratic. Therefore, it is important to keep in mind that influencing behaviour, even under ideal conditions, is an ethically ambiguous act (Kelman 1965).

If researchers decide to aim at attitudinal or behavioural change, there are different levels at which they could try to impose this change. Chen et al. (2008) rightfully argued that a dilemma exists between *enforcement* and *protection* of personal information. According to Kelman, Warwick, and Bermant (1978), the goals of an intervention range from coercion, via manipulation and persuasion, to facilitation of a certain attitude or behaviour. These different means of intervention are extensively described by Kelman (2001). He states that *coercion* implies that people are forced to take actions that contradict their preferences. Examples of coercive solutions are parents who forbid their children to use SNSs, censorship of certain posts by SNS filters, or SNS systems that do not allow minors to post publicly on their SNS profile. *Manipulation* entails a change in the structure of alternatives that users get, for example by making certain privacy settings in SNSs the default. This leaves the person free to make choices, but within a deliberately modified structure. The next point on the continuum that Kelman (2001) describes is *persuasion*, which is built on the strength of argumentation, reasoning, and debate to influence people's attitudes and behaviour. Different privacy-awareness-raising campaigns and privacy-enhancing awareness tools can be categorised as a form of persuasion, as they try to explain why you should not post certain information (rather than just inform about the risks, e.g. pedagogy of regret, see Brown 2012). Finally, Kelman (2001) defines *facilitation* as a technique that focuses on offering different resources. With regard to privacy interventions, examples are awareness-raising campaigns (making information available) that do not try to convince people to act a certain way, but that offer different tools and strategies that can be used whenever users choose to use them.

This continuum shows a gradual increase in the freedom that the person being influenced still has. Persuasion and facilitation are generally seen as consistent with the principle of autonomy and freedom, and are therefore ethically more acceptable than coercion and manipulation. However, this does not mean that facilitation is always ethically justifiable, or that coercion is never ethically justifiable (Kelman 2001). Indeed, facilitation by offering certain tools (and not others) might already structure people's choices and limit options. Furthermore, offering options to certain groups, but not to others, can be seen as a coercion of the others, as they do not have the resources available. On the other hand, coercion can be ethically justifiable, for instance when public health or public security is seriously threatened. Again, this can be seen in the light of the discussion above, concerning whether privacy is regarded as a human right (is a violation of privacy rights a serious threat to public health or safety?) or as a property right.

We argue that it is necessary for a researcher to be transparent about his or her values and norms when setting the goals of any solution and when deciding on how to reach these goals.

2.5. Q5. Who is the target audience?

The previous two questions about awareness, attitudes, and behaviour also need to be considered in the light of the target audience. While researchers sometimes take into account their target audience when it comes to problem analysis or design, they should also take into account their target audience with regard to the ethical question of influencing awareness, attitudes, and behaviour. The importance of this consideration becomes apparent when vulnerable audiences, such as minors, are concerned. Recent research shows that SNSs are increasingly popular with teenagers, who are sharing ever more personal information on these sites (Madden et al. 2013). The privacy concerns that are associated with this increase raise the question whether we need to protect these users, especially since several studies show that these teenagers might be particularly vulnerable in terms of their online privacy (Walrave and Heirman 2013).

To reach all minors, school education has been put forth as a solution (Patchin and Hinduja 2010; Tejedor and Pulido 2012; Vanderhoven, Schellens and Valcke 2014b) and a variety of educational tools has been developed to meet these concerns (e.g. Insafe 2012; Vanderhoven, Schellens and Valcke 2014a). However, for most of these materials, it is not clear whether they only aim to raise awareness, to enhance skills, or whether they aim to change attitudes and behaviour as well.

Although there might be ethical objections to influencing teenagers' attitudes and behaviours (e.g. the hierarchical relationship that arises when trying to influence minors), there are other important

considerations to take into account, such as developmental skills. Can we expect that a teenager is able to make *good* decisions when disclosing information in SNSs? It has been found that young users are more impatient, and are less likely to recognise the risks and future consequences of their decisions (Cauffman and Steinberg 2000). The technical properties of SNSs (e.g. scalability, see boyd 2008a) make it difficult for users to revise their decisions and increase the impact of certain decisions. Hence, when a teenager for example shares a photograph on a SNS in which he/she is drinking alcohol, he/she might have the beneficial short-term consequences in mind: it might be considered *cool* by his or her peers and it might shape this teenager's identity in a way that he/she perceives as beneficial. However, it can be harder for this teenager to recognise the possible future consequences of posting this picture, for example on future job applications. Since it was also found that teenagers have a harder time controlling their impulses and have higher thrill-seeking and disinhibition scores than adults (Cauffman and Steinberg 2000), this example might not be a rare case. The personality of minors may simply not be evolved enough to make good and informed decisions.

We believe that it is important for researchers to deliberately consider the characteristics of the group of people they research and for whom they develop and propose artefacts, tools, and interventions.

3. Discussion

3.1. Summary and reflections

Researchers and their solutions for privacy problems in SNSs are not neutral: ideas, norms, and values of the researchers are translated into problem definition as well as solution, and the developed solution delegates instructions on how to act (Latour 1992). In this paper, we argue for making the privacy research process more transparent by asking self-reflective questions throughout the process.

We first argued that a researcher should take into account which actors are involved when defining the privacy problem. The first question has two sub-questions: (a) is the privacy problem defined by security experts or users and (b) does it concern relationships towards other people or towards institutions? This first question is necessary because the vocabulary, solutions, and challenges are different. The second question concerned the definition of privacy as a human right or as a property right on one's data. We consider it necessary for researchers to 'take a stance' and question and formulate their perspective on this continuum. If not, solutions are justified via the researchers' unstated assumptions, and social, economical, and political agendas remain hidden. The third and fourth questions centred on the desired impact of the solution (i.e. increasing awareness, and changing attitudes and behaviours). Although raising awareness might seem self-evident, it can also have negative outcomes, is not always possible, and is never neutral. Influencing attitudes and behavioural change is even more problematic because in addition to imposing one's own notion of privacy, it also pushes users into a certain direction that is perceived as desirable. It is therefore necessary that a researcher justifies why, how, and to what extent he or she wants to influence the user. Finally, we argued that a researcher should take into account the target audience when developing solutions, because certain audiences, such as minors, are more vulnerable than others.

Taken together, all of these questions make the research process more transparent, including the role of the researcher and the ethical and moral dimension of the solution being built. It should be noted, however, that our approach also has limitations. First, in this article, we have discussed the ethical dimension from a general perspective. Further work could elaborate how different philosophical orientations towards ethics relate to transparency and self-reflection, like virtue ethics (Verbeek 2011; Brey, Briggle, and Spence 2012). Second, we should not forget that transparency and self-reflection are not ends in themselves, and that while they may be necessary for making progress towards our 'real' goal of improving privacy, they may not be sufficient. To make progress, we need practical procedures for engendering self-reflection, we need practical procedures for then transforming it into manifest changes to help privacy, and we need evaluation methods to test whether we have reached our goals. In the next and final subsection of this paper, we will sketch such practical procedures for transformation. For now, we rely on the evaluation methods that have been proposed for privacy-enhancing technologies – noting that these evaluation methods will be a next frontier to be targeted in future work.

3.2. Practical implications

How can a researcher or someone interested in subjecting their work to these self-reflective questions proceed? We hope that a cognitive awareness of the issues raised can be a first step in this process. However, we also believe that it is better to draw on multiple perspectives (when the non-uniqueness of perspectives is the central issue), and better still to complement cognition by action. We therefore believe that procedures that aim

at overcoming an overly strong focus on a single 'solution' by eliciting different viewpoints can be helpful. In Morton et al. (2013), we have proposed the idea of *tool clinics* as a format for doing this. We believe that the lead questions identified in the present paper and their discussion can help structure such a tool clinic. In order to explain how, we will first give some background on the general concept.

Tool clinics aim at encouraging a collaborative (re-) consideration of a technological solution, research technique, or other artefact, in order to critically assess its design, development, and deployment from multiple perspectives. Another objective is to turn such solutions or artefacts into a tool for exploring the problem space. Finally, a tool clinic can be used to provide those who are developing the solutions with a setting to rethink the framing and presentation of their solutions.

A tool clinic provides a framework and approach for multiple-perspective formative exploration and review of a technological solution, research technique, or other artefact under development. The objective is to reflect from different perspectives on practices around the development, encoding, use, domestication, decoding, and sustainability of a tool to gain quasi-ecological validation. Practically, we think of a tool clinic in terms of a structured meeting or a series of meetings (not necessarily face-to-face) between an appropriately composed group of researchers and practitioners with different disciplinary, stakeholder-related, etc., backgrounds.

The idea of a tool clinic is related to a range of formats from education, the military, software development, and science and technology studies (see Morton et al. 2013 for more details and references). Inspired by this work, we preview a typical tool clinic to consist of three steps:

1. Identifying particular affordances of the technological solution, research technique, or other artefact and possible (unintended) consequences for people and society;
2. Gathering perspectives and practices of different experts, disciplines, and/or stakeholders (users, policy-makers, industry, etc.) linked with the development, deployment, and sustainable evolution of a particular tool, solution, technique, or artefact;
3. Informing and advising on the technological design of the tool or solution, in order to avoid negative consequences and to further positive outcomes.

The self-reflective questions described and discussed in the present paper can serve as an essential backdrop for identifying one's own perspective and the affordances of one's artefact in step 1, as well as for the selection of experts in step 2 (and in turn the elicitation of their perspectives). Of course, tool clinics are not exempt from the processes that we have discussed in this paper. For example, they may themselves create new and narrowing research norms (which should be reflected upon). Still, a structure such as a tool clinic could do a lot to help researchers over the threshold towards explicit reflection and deliberation, processes that often get lost in the time pressures of standard research practices and informal feedback cultures.

Notes

1. The name of the project is omitted for the purpose of double-blind reviewing.
2. Latour (1992) proposed to conceive technologies as humans with whom we interact and shape our everyday actions. When designers develop technologies, they delegate certain tasks that were previously assigned to humans or other technologies. In turn, these technologies impose certain behaviours on humans, and they delegate prescription, that is, instructions on how to act, and thereby the moral and ethical dimension of technologies.
3. It should be noted that security experts, of course, can also be users and express social privacy-related problems. Users may also express their concern towards information gathering and processing. Moreover, both institutional and social privacy are strongly intertwined. For example, third parties need to adopt users' information in a manner that is consistent with the privacy policy and users' privacy preferences. To unravel the complexity of online privacy, however, we find it is necessary to reduce complexity and differentiate between the actors and relationships involved.
4. Samuelson (2000) gives a good summarization of these positions and outlines some problems with them.
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
6. Foucault ([1976] 1979), for example, questioned self-alienation when arguing that the age of reason forces people to be reflective all of the time. Internalizing such an idea leads to a constant questioning of one's own behaviour and makes people think about their own actions, rather than act in the first place.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the IWT [100048]. The research leading to these results has received funding from the Strategic Basic Research (SBO) Program of the Flemish Agency for

Innovation through Science and Technology (IWT) in the context of the SPION project under grant agreement number 100048.

References

Acquisti, Alessandro, and Ralph Gross. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." In *Privacy Enhancing Technologies*, edited by George Danezis and Phillippe Golle, 36–58. Berlin: Springer.

Agre, Philip, and Marc Rotenberg. 2001. *Technology and Privacy: The New Landscape*. Cambridge: MIT Press.

Altman, Irvin. 1976. "Privacy: A Conceptual Analysis." *Environment and Behavior* 8 (1): 7–29.

Bauman, Zygmunt, and David Lyon. 2013. *Liquid Surveillance*. Cambridge: Polity Press.

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. 2005. "Privacy in E-commerce: Stated Preferences vs. Actual Behavior." *Communications of the ACM* 48 (4): 101–106.

Bernstein, Michael, Eytan Bakshy, Moira Burke, and Brian Karrer. 2013. "Quantifying the Invisible Audience in Social Networks." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 21–30. New York: ACM.

boyd, danah. 2008a. "Taken Out of Context: American Teen Sociality in Networked Publics." PhD diss., University of California–Berkeley, School of Information, CA.

boyd, danah. 2008b. "Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence." *Convergence: The International Journal of Research into New Media Technologies* 14 (1): 13–20. doi:10.1177/1354856507084416.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. 2012. "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science* 4: 340–347. doi:10.1177/1948550612455931.

Brey, Philip, Adam Briggle, and Edward Spence. 2012. *The Good Life in a Technological Age*. New York: Routledge.

Brown, Rebecca. 2012. "The Pedagogy of Regret: Facebook, Binge Drinking and Young Women." *Continuum-Journal of Media & Cultural Studies* 26 (3): 357–369. doi:10.1080/10304312.2012.665834.

Cauffman, Elizabeht, and Laurance Steinberg. 2000. "(Im) maturity of Judgment in Adolescence: Why Adolescents may be Less Culpable than Adults." *Behavioral Sciences & the Law* 18 (6): 741–760. doi:10.1002/bsl.416.

Chen, Houn-Gee, Charlie Chen, Louis Lo, and Samuel Yang. 2008. "Online Privacy Control via Anonymity and Pseudonym: Cross-cultural Implications." *Behaviour and Information Technology* 27 (1): 229–242.

Coté, Marc, and Jennifer Pybus. 2007. "Learning to Immaterial Labour 2.0:MySpace and Social Networks." *Ephemera: Theory & Politics in Organization* 7 (1): 88–106.

De Hert, Paul. 2012. "Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law." In *Managing Privacy Through Accountability*, edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland, and Hector Postigo, 193–232. Bastingstoke: Palgrave Macmillan.

Foucault, Michel (1979) [1976]. *The History of Sexuality Volume 1: An Introduction*. London: Allen Lane.

Fuchs, Christian. 2012. "The Political Economy of Privacy on Facebook." *Television & New Media* 13 (2): 139–159. doi:10.1177/1527476411415699.

Gandy, Oscar. 2003. "Data Mining and Surveillance in the Post-9/11 Environment." In *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, edited by Kristie Ball and Frank Webster, 26–41. Sterling, VA: Pluto Press.

Giddens, Anthony. 1991. *The Consequences of Modernity*. Stanford, CA: Stanford University Press.

Gillespie, Tarleton, Pablo Boczkowski, and K. A. Foot. 2014. *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, Massachusetts: MIT Press.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

Gürses, Seda, and Claudia Diaz. 2013. "Two Tales of Privacy in Online Social Networks." *IEEE Security & Privacy* 11 (3): 29–37. doi:10.1109/MSP.2013.47.

Hackett, Edward, Olga Amsterdamska, Michael Lynch, and Judy Wajcman. 2008. "Introduction." In *The Handbook of Science and Technology Studies (3rd)*, edited by Edward Hackett, Olga Amsterdamska, Michael Lynch, and Judy Wajcman, 1–7. Cambridge: MIT Press.

Insafe. 2012. "Educational Resources for Teachers." Retrieved from http://www.saferinternet.org.

Kelman, Herbert. 1965. "Manipulation of Human Behavior: An Ethical Dilemma for the Social Scientist." *Journal of Social Issues* 21 (2): 31–46. doi:10.1111/j.1540-4560.1965.tb00494.x.

Kelman, Herbert. 2001. "Ethical Limits on the Use of Influence in Hierarchical Relationships." In *Social Influences on Ethical Behavior in Organizations*, edited by John Darley, David Messick, and Tom Ryler, 11–20. Mahwah, NJ: Lawrence Erlbaum.

Kelman, Herbert, Donald Warwick, and G. Bermant. 1978. "The Ethics of Social Intervention: Goals, Means, and Consequences." In *The Ethics of Social Intervention*, 3–33. New York: Wiley.

Kimmel, Allan. 1988. *Ethics and Values in Applied Social Research*. London: Sage.

Knijnenburg, Bart, Alfred Kobsa, and Hongxia Jin. 2013. "Preference-based Location Sharing: Are More Privacy Options Really Better?" In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2667–2676. New York: ACM.

Latour, Bruno. 1992. "Where are the Missing Masses? The Sociology of a Few Mundane Artifacts." In *Shaping Technology/ Building Society: Studies in Sociotechnical Change*, edited by Wiebe Bijker and John Law, 225–258. Cambridge, MA: MIT Press.

Litt, Eden. 2013. "Understanding Social Network Site Users' Privacy Tool Use." *Computers in Human Behavior* 29 (4): 1649–1656.

Lohmann, Larry. 2013. "Performative Equations and Neoliberal Commodification: The Case of Climate." In *Nature Inc.: Environmental Conservation in the Neoliberal age*, edited by Bram Büschler, Wolfram Dressler, and Robert Fletcher, 158–180. University of Arizona Press.

Madden, Mary, Aamanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaton. 2013.

"Teens, Social Media, and Privacy (No. PEW Report)." http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

Markham, Annette. 2013. "The Dramaturgy of Digital Experience." In *The Drama of Social Life: A Dramaturgical Handbook*, edited by Charles Edgley, 279–293. Burlington, VT: Ashgate Press.

Martin, Nigel, John Rise, and Robin Martin. 2015. "Expectations of Privacy and Trust: Examining the Views of IT Professionals." *Behaviour and Information Technology* 35 (6): 500–510.

Morton, Anthony, Bettina Berendt, Seda Gürses, and Jo Pierson. 2013. "'Tool Clinics' – Embracing Multiple Perspectives in Privacy Research and Privacy-sensitive Design." *Dagstuhl Reports* 3 (7): 96–104.

Mun, Min, Shuai Hao, Nilesh Mishra, Katie Shilton, Jeff Burke, Deborah Estrin, Mark Hansen, and Ramesh Govindan. 2010. "Personal Data Vaults: A Locus of Control for Personal Data Streams." In *Proceedings of the 6th International Conference*. New York: ACM, 17:1–17:12.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79 (1): 101–158.

Papacharissi, Zizi. 2012. "Afterword: A Remediation of Theory." In *Produsing Theory in a Digital World*, edited by Rebecca An Lind, 195–203. New York: Peter Lang International Academic.

Patchin, Justin, and Sameer Hinduja. 2010. "Changes in Adolescent Online Social Networking Behaviors from 2006 to 2009." *Computers in Human Behavior* 26 (6): 1818–1821. doi:10.1016/j.chb.2010.07.009.

Petronio, Sandra. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: New York Press.

Purtova, Nadezhda. 2010. "Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights." *Netherlands Quarterly of Human Rights* 28 (2): 179–198.

Raynes-Goldie, Kate. 2010. "Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook." *First Monday* 15 (1). http://firstmonday.org/ojs/index.php/fm/article/view/2775.

Rouvroy, Antoinette, and Yves Poullet. 2009. "The Right to Informational Self-determination and the Value of Self-development: Reassessing the Importance of Privacy for Democracy." In *Reinventing Data Protection?* edited by Serge Gutwirth, 45–76. Amsterdam, The Netherlands: Springer.

Warren, Samuel, and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4: 193–220.

Samuelson, Pamela. 2000. "Privacy as Intellectual Property?" *Stanford Law Review* 52 (52): 1125–1173.

Solove, Daniel. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3): 477–560.

Stutzman, Fred, Ralph Gross, and Alessandro Acquisti. 2013. "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook." *Journal of Privacy and Confidentiality* 4 (2): 7–41.

Tejedor, Santiago, and Christina Pulido. 2012. "Challenges and Risks of Internet Use by Children. How to Empower Minors?" *Comunicar* 20 (39): 65–72. doi:10.3916/C39-2012-02-06.

Vanderhoven, Ellen, Tammy Schellens, and Martin Valcke. 2014a. "Educational Packages about the Risks on Social Network Sites: State of the Art." *Procedia – Social and Behavioral Sciences* 112 (112): 603–612. doi:10.1016/j.sbspro.2014.01.1207.

Vanderhoven, Ellen, Tammy Schellens, and Martin Valcke. 2014b. "Exploring the Usefulness of School Education about Risks on Social Network Sites: A Survey Study." *The Journal of Media Literacy Education* 5 (1): 285–294.

Verbeek, Peter-Paul. 2011. *Moralizing Technology: Understanding and Designin the Morality of Things*. Chicago, IL: University of Chicago Press.

Walrave, Michel, and Wannes Heirman. 2013. "Adolescents, Online Marketing and Privacy: Predicting Adolescents' Willingness to Disclose Personal Information for Marketing Purposes." *Children & Society* 27 (6): 434–447. doi:10.1111/j.1099-0860.2011.00423.x.

Wang, Yang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Leon, and Lorrie Cranor. 2011. "'I Regretted the Minute I Pressed Share': A Qualitative Study of Regrets on Facebook." In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. New York: ACM, 10:1–10:16.

Waskul, Dennis. 2005. "Ekstasis and the Internet: Liminality and Computer-mediated Communication." *New Media & Society* 7 (1): 47–63. doi:10.1177/1461444805049144.

Westin, Alan. 1967. *Privacy and Freedom*. New York: Atheneum.

Williams, Robin, and David Edge. 1996. "The Social Shaping of Technology." *Research Policy* 25: 865–899.

Xu, Heng. 2012. "Reframing Privacy 2.0 in Online Social Networks." *University of Pennsylvania Journal of Constitutional Law* 14 (4): 1077–1102.